

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年10月 8日

出 願 番 号

Application Number:

特願2002-294375

[ST.10/C]:

[JP2002-294375]

出 願 人

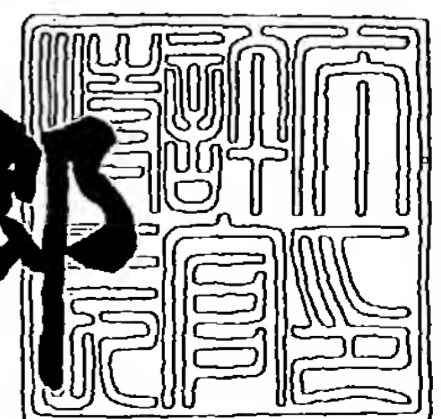
Applicant(s):

株式会社日立製作所

2003年 6月18日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



【書類名】 特許願

【整理番号】 K02009411A

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明者】

 【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 ビジネスソリューション事業部内

 【氏名】 有坂 剛

【発明者】

 【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 ビジネスソリューション事業部内

 【氏名】 近藤 香

【発明者】

 【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 ビジネスソリューション事業部内

 【氏名】 紅山 伸夫

【発明者】

 【住所又は居所】 神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所 ビジネスソリューション事業部内

 【氏名】 小池 博

【発明者】

 【住所又は居所】 神奈川県横浜市戸塚区戸塚町 5 0 3 0 番地 株式会社日立製作所 ソフトウェア事業部内

 【氏名】 小俣 光輝

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子商取引方法

【特許請求の範囲】

【請求項 1】

ネットワークで接続された2台以上の情報処理装置間で、電子文書をやり取りする電子商取引方法において、

電子文書を送信する装置は、電子文書データを暗号化し、電子文書データを加工し、前記暗号化した電子文書データと前記加工した電子文書データをパッケージ化して送信し、

電子文書を受信する装置は、受信したデータを加工した電子文書データと暗号化した電子文書データにアンパッケージ化し、前記加工した電子文書データを復元し、前記暗号化した電子文書データを復号化し、前記復元した電子文書データと前記復号化した電子文書データが一致するか否かを判定することを特徴とする電子商取引方法。

【請求項 2】

少なくとも2台の装置に共通する雛形データを備え、前記電子文書を送信する装置は、電子文書データを加工する際に電子文書データと雛形データの差分情報を抽出し、前記電子文書を受信する装置は、加工した電子文書データを復元する際に前記雛形データと前記差分情報を合成することを特徴とする請求項 1 記載の電子商取引方法。

【請求項 3】

電子文書データを加工する際に差分情報を圧縮し、加工した電子文書データを復元する際に圧縮された差分情報を伸長することを特徴とする請求項 2 記載の電子商取引方法。

【請求項 4】

前記電子文書を送信する装置は、電子文書データを加工する際に電子文書データを圧縮し、前記電子文書を受信する装置は、加工した電子文書データを復元する際に圧縮された電子文書データを伸長することを特徴とする請求項 1 記載の電子商取引方法。

【請求項 5】

電子文書データを暗号化する際に電子文書データのメッセージダイジェストを算出し、前記電子文書データのメッセージダイジェストを暗号化し、復元した電子文書データと復号化した電子文書データが一致するか否かを判定する際に復元した電子文書データのメッセージダイジェストを算出し、前記算出したメッセージダイジェストと前記復号化したメッセージダイジェストとが一致するか否かを判定することを特徴とする請求項 1 記載の電子商取引方法。

【請求項 6】

少なくとも 2 台の装置に共通する雛形データを備え、前記電子文書を送信する装置は、電子文書データを加工する際に電子文書データと雛形データの差分情報を抽出し、前記電子文書を受信する装置は、加工した電子文書データを復元する際に前記雛形データと前記差分情報を合成することを特徴とする請求項 5 記載の電子商取引方法。

【請求項 7】

電子文書データを加工する際に差分情報を圧縮し、加工した電子文書データを復元する際に圧縮された差分情報を伸長することを特徴とする請求項 6 記載の電子商取引方法。

【請求項 8】

前記電子文書を送信する装置は、電子文書データを加工する際に電子文書データを圧縮し、前記電子文書を受信する装置は、加工した電子文書データを復元する際に圧縮された電子文書データを伸長することを特徴とする請求項 5 記載の電子商取引方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は電子文書を用いた電子商取引方法に係り、特にネットワーク環境で分散した担当者間で電子文書を通信させながら業務を進めるのに好適な電子商取引方法に関する。

【 0 0 0 2 】

【従来の技術】

発注者から受注者へ発注書を電子文書として送信し、受注者がそれを見て業務を行うような電子商取引において、発注書が発注者によって作成されたものであり、改竄やなりすましが無いことを、受注者や第三者によって推定できることが望まれている。この課題はいわゆる電子署名法のもと、公開鍵暗号方式などの暗号技術に応用した電子署名技術を用いて、発注者が発注書に電子署名を付すことで解決されるようになった（例えば、特許文献1参照）。

【0003】

一方、Web-EDIのような電子商取引においては、データ送信量削減のため、オリジナルに対する差分を送信し、受注者はオリジナルと差分とから得られた発注情報を用いて業務を行っている。この取引では、差分情報の受信者である受注者側のシステムで、オリジナルと差分とから発注情報を生成することを、発注者と受注者の間で予め合意することが前提となっている。この合意を支援するために、送信側及び受信側のシステムで、通信路の暗号化や送受信したデータの厳重な管理を行っている。このような差分情報をやり取りする電子商取引に電子署名技術を利用しようとする場合、差分情報に電子署名を付して送信することが考えられる。電子署名技術により、受注者や第三者は、差分情報が発注者によって作成されたデータであることを推定できる。

【0004】

しかし、オリジナルが改竄されてしまった場合や、オリジナルと差分とから得た受注情報が改竄された場合は、発注者の意図とは異なる情報によって業務が遂行されてしまうため、何らかの被害が出ることが想定される。この場合、電子署名法では、あくまで差分情報が発注者によって作成されたものと推定できることしか言えないため、情報の改竄は電子署名法の適用範囲を超えた問題となる。例えば、悪意のある受注者が、オリジナルの発注品項目の単位をg(グラム)からkg(キログラム)に改竄した場合、オリジナルと差分とから作られた発注情報は、発注者の意図したものではなくなるため、発注者が被害を蒙ることとなる。この場合、誰が改竄したのか、電子商取引システムの欠陥なのか、などが争われることとなる。

【0005】

【特許文献1】

特開2002-91303号公報

【0006】

【発明が解決しようとする課題】

上記のように、従来の電子署名技術では、単純に差分に電子署名を付した場合は、受信者は差分が送信者によって作成されたことしか推定できないため、生成した電子文書に対する署名検定が行えない。

【0007】

本発明の目的はオリジナルに対する差分情報をやりとりする電子商取引において、オリジナルと差分情報とからの得られる情報が送信者によって作成されたことを、受信者や第三者によって推定できる電子商取引方法を提供することである。

【0008】

【課題を解決するための手段】

電子文書の改竄やなりすましを防ぎつつ、差分情報を送信することでデータ転送量を削減するために、2台の装置に共通する雛形データを予め記憶し、電子商取引ではオリジナル情報から、雛形データを除く部分を差分情報として生成する。データを送信する装置は、オリジナル情報を暗号化し、差分情報を生成し、暗号化したオリジナル情報と差分情報をパッケージ化して送信する。データを受信する装置は、受信したパッケージ化されたデータをアンパッケージし、差分情報と雛形データからオリジナル情報を復元し、暗号化したデータを復号化し、復号化したデータと復元したオリジナル情報が一致するか否かを判定する。

【0009】

【発明の実施の形態】

以下、本発明の実施例を図面に基づいて説明する。

【0010】

図13を用いて本実施例における業務の内容を説明する。本発明では、2台以上（ここでは2台）の業務処理装置1，2をネットワークで物理的に接続されて

いる環境下で、複数の業務担当者が電子文書へのデータの入力などの業務を行っている。ここでは受発注業務において、業務処理装置1では発注業務担当者が発注書を作成し、発注書を受信した受注業務担当者が、受信した発注書は発注業務担当者によって作成されたものであることが確認できるようにするため、発注書に暗号化を施してから受注業務担当者へ発注書を送付する。

【 0 0 1 1 】

業務処理装置2ではインターネットを介して発注書を受信後、このデータを復号化し、業務処理装置1と2の間でのデータ不整合や転送後のデータ改竄がない、つまり、確かに発注業務担当者によって作成された発注書であることを受注業務担当者が確認したのち、この発注書を基に受注業務を行う。

【 0 0 1 2 】

業務処理装置1, 2に共通する雛形文書を予め記憶し、秘密鍵に対応する公開鍵は業務処理装置2のハードディスク上に格納されている。

(1) 業務処理装置1において、発注業務担当者は、発注書の差分（例えば発注する商品型番・個数など）と、どの雛型文書かを識別する雛型IDとを入力する。

(2) 上記(1)で得た差分と雛型IDから、バイナリのデータ列である差分情報を生成する。

(3) 上記(1)で入力した雛型IDから雛型文書を特定して、これを差分とマージして注文情報を生成する。

(4) 上記(3)で作った注文情報に対するダイジェストを計算し、このダイジェストを発注者の秘密鍵を使って暗号化して電子署名を生成する。

(5) 上記(2)で生成した差分情報と、上記(4)で生成した注文情報に対する電子署名とをパッケージングして、業務処理装置2に送信する。

(6) 業務処理装置2は、上記(5)で送られてきた情報をアンパッケージングし、差分情報と電子署名とに分割する。

(7) 上記(6)で得た差分情報から、差分と雛型IDを抽出し、雛型IDから雛型文書を特定し、これを差分とマージして注文情報を生成する。

(8) 上記(6)で得た電子署名を発注業務担当者の公開鍵を使って復号化する

（９）上記（７）で生成した注文情報のダイジェストを計算し、これが上記（８）で得た値と一致するかどうかを調べて署名の検定を行う。

（１０）業務処理装置２では、検証された注文情報を受注業務担当者に出力する。

【 0 0 1 3 】

本発明の電子商取引方法では、注文情報に対応して発注業務担当者の電子署名が存在し、（８）によって、業務処理装置２では、この注文情報が発注業務担当者によって作成されたことを推定できる。また、（６）で得た電子署名と、（７）で生成した注文情報とを組にして出力することで、受信業務担当者や第三者が発注業務担当者の公開鍵を使って、注文情報が発注業務担当者によって作成されたことを推定できる。

【 0 0 1 4 】

本実施例のハードウェアの構成を、図２を用いて説明する。

【 0 0 1 5 】

業務処理装置１は、電子文書の発行業務に必要なディスプレイ１１、キーボード１２、マウス１３、フロッピーディスク駆動装置１４、フロッピーディスク２９、ハードディスク１５、メインメモリ１６及びＣＰＵ１７からなるハードウェアを備える。ディスプレイ１１、キーボード１２、マウス１３、フロッピーディスク駆動装置１４、ハードディスク１５及びメインメモリ１６は、ＣＰＵ１７よりバス１８を介してアクセスされる。フロッピーディスク２９は、フロッピーディスク駆動装置１４を介してアクセスできる。業務処理装置１は、サーバ１９を介してインターネット２０と接続される。

【 0 0 1 6 】

業務処理装置２は、受注業務に必要なディスプレイ２１、キーボード２２、マウス２３、ハードディスク２４、メインメモリ２５及びＣＰＵ２６を備える。ディスプレイ２１、キーボード２２、マウス２３、ハードディスク２４及びメインメモリ２５は、ＣＰＵ２６よりバス２７を介してアクセスされる。業務処理装置２は、サーバ２８を介してインターネット２０と接続される。

【 0 0 1 7 】

図 1 を用いて、本実施例のソフトウェアの構成を説明する。業務処理装置 1 のメインメモリ 1 6 には、業務処理装置 1 を制御する全体制御プログラム 1 6 0 が常にロードされている。発注業務を行う場合は、さらに、発注業務制御プログラム 1 6 1、発注データ作成プログラム 1 6 2、送信データ生成制御プログラム 1 6 3 及び発注データ送信プログラム 1 6 4 がメモリ 1 6 にロードされる。送信データ生成制御プログラム 1 6 3 は、注文情報生成プログラム 1 6 3 1、注文情報暗号化プログラム 1 6 3 2、差分情報生成プログラム 1 6 3 3、圧縮処理プログラム 1 6 3 4 及び送信データ生成プログラム 1 6 3 5 から構成される。

【 0 0 1 8 】

また、本実施例では、発注業務を実施する前に、暗号化に必要な秘密鍵および公開鍵を準備する必要がある。秘密鍵および公開鍵は、証明書認証局などの他者によって作成（発行）できるが、この場合は証明書認証局などへの使用料の支払いが必要となるため、本実施例では業務処理装置 1 が秘密鍵及び公開鍵を作成する。業務処理装置 1 のメインメモリ 1 6 には、鍵生成システムとして、鍵生成処理制御プログラム 1 6 5、鍵生成プログラム 1 6 5 1、利用者 ID 登録プログラム 1 6 5 2、秘密鍵 FD 作成プログラム 1 6 5 3 及び公開鍵ファイル作成プログラム 1 6 5 4 が一時的にロードされる。ワークエリア 1 6 6 は、常に確保される。ハードディスク 1 5 には、商品 DB 1 5 1、レイアウト情報格納 DB 1 5 2、業務履歴 DB 1 5 3 及び電子文書データ蓄積 DB 1 5 4 が格納される。秘密鍵（暗号化鍵）ファイル 3 0 は、フロッピーディスク 2 9 に格納され、フロッピーディスク駆動装置 1 4 を介して参照される。

【 0 0 1 9 】

業務処理装置 2 のメインメモリ 2 5 には、業務処理装置 2 を制御する全体制御プログラム 2 5 0 が常にロードされている。受注業務を行う場合は、受注業務制御プログラム 2 5 1、受注データ受信プログラム 2 5 2、受信データ解析制御プログラム 2 5 3 及び受注処理実行プログラム 2 5 4 がメインメモリ 2 5 にロードされる。受信データ解析制御プログラム 2 5 3 は、受信データ分割プログラム 2 5 3 1、注文情報生成プログラム 2 5 3 2、注文情報復号化プログラム 2 5 3 3

、圧縮復元プログラム 2 5 3 4 及び署名検定プログラム 2 5 3 5 から構成される。ワークエリア 2 5 5 は常に確保される。ハードディスク 2 4 には、公開鍵ファイル 4 0、レイアウト情報格納 DB 2 4 2 及び電子文書データ蓄積 DB 2 4 4 が記憶される。

【 0 0 2 0 】

以上述べたハードウェア・ソフトウェアの構成の下で発注業務処理が行なわれる。業務処理装置 1 のハードディスク 1 5 に格納されるレイアウト情報格納 DB 1 5 2 と業務処理装置 2 のハードディスク 2 4 に格納されるレイアウト情報格納 DB 2 4 2 のそれぞれの内容は同一である。また、業務処理装置 1 で使用する秘密鍵ファイル 3 0 に対応する公開鍵ファイル 4 0 は、業務処理装置 2 のハードディスク 2 4 に格納される。

【 0 0 2 1 】

業務処理装置 1 では、発注業務制御プログラム 1 6 1 が発注データ作成プログラム 1 6 2 を起動し、業務担当者から発注書発行に必要なデータを入力させ（図 1 3 の（1））、注文情報を生成する（図 1 3 の（3））。ネットワーク上でのデータの改竄の有無を検証する場合、注文情報あるいは注文情報の一部と、注文情報を暗号化したものとをパッケージして送信し、受信側で、受信データをアンパッケージし、注文情報あるいは注文情報の一部と復号化した注文情報とを比較する。注文情報の作成終了後、注文情報あるいは注文情報の一部と、注文情報を暗号化したものとをパッケージするまでの一連の処理の制御を行う送信データ生成制御プログラム 1 6 3 を起動する。

【 0 0 2 2 】

データを暗号化するとデータ量が増加し、通信に多大な負荷がかかるので、暗号化する対象のデータのメッセージダイジェストを求め、このメッセージダイジェストに対して暗号化することが行われる。メッセージダイジェストとは、ハッシュ関数という特別な関数を使って、任意の文字列から、決められた範囲の整数を生成した値である。ハッシュ関数は一方向関数であり、例えば SHA-1、MD5 などがある。メッセージダイジェストから元のデータを復元することは出来ない。また、ハッシュ関数は、入力データが 1 b i t でも異なると、値が大きく

異なったダイジェストを生成するので、元ファイルのダイジェストを保存しておくことで、そのファイルに変更が加えられたか否かを確認できる。メッセージダイジェストの暗号化は、元ファイルそのものを保存する方法よりもデータ量が節約でき、さらに改竄の検知も容易であるという特徴がある。

【 0 0 2 3 】

メッセージダイジェストを暗号化する場合は、注文情報生成プログラム 1 6 3 1 により、発注データ作成プログラム 1 6 2 によって作成された注文情報のメッセージダイジェストを求める（図 1 3 の（4））。注文情報暗号化プログラム 1 6 3 2 は、秘密鍵ファイル 3 0 を用いて注文情報を暗号化する（図 1 3 の（4））。注文情報の一部のみをパッケージする場合は、差分情報生成プログラム 1 6 3 3 によって、発注業務処理に必要な情報のみを差分情報として抽出し（図 1 3 の（2））、必要であれば圧縮処理プログラム 1 6 3 4 を用いて、注文情報あるいは注文情報の一部に対して圧縮処理を施す。送信データ生成プログラム 1 6 3 5 によって、注文情報あるいは差分情報と、暗号化したデータとをパッケージングし、発注データ送信プログラム 1 6 4 によって、受注業務処理を行う業務処理装置 2 へパッケージングした結果を送信する（図 1 3 の（5））。

【 0 0 2 4 】

業務処理装置 2 では受注業務処理が行なわれる。受注業務制御プログラム 2 5 1 は、受注データ受信プログラム 2 5 2 を常時起動状態にしており、データを受信すると、受信データ解析制御プログラム 2 5 3 を起動する。送られてきたデータを、受信データ分割プログラム 2 5 3 1 によって、注文情報あるいは差分情報と暗号化データとに分割し（図 1 3 の（6））、注文情報生成プログラム 2 5 3 2 によって、差分情報の場合は差分情報を元にして注文情報を生成し（図 1 3 の（7））、注文情報復号化プログラム 2 5 3 3 によって公開鍵を用いて暗号化されたデータを復号化する（図 1 3 の（8））。データが圧縮されている場合は圧縮復元プログラム 2 5 3 4 によって圧縮データを復元し、署名検定プログラム 2 5 3 5 によって復号化したデータと注文情報との比較を行う。復号化したデータがメッセージダイジェストの場合は、注文情報のメッセージダイジェストを求め、これと復号したメッセージダイジェストとを比較し、双方が一致した場合は注

文情報が確かに発注業務担当者によって作成されたものであると判断し（図 1 3 の（9））、送られてきた注文情報に対する受注業務が可能となり、受注業務担当者は受注処理実行プログラム 2 5 4 を起動する（図 1 3 の（10））。

【0025】

本実施例で使用するデータの暗号化及び復号化を説明する。データの暗号化及び復号化では、暗号化と復号化とでそれぞれ異なる鍵を用いる公開鍵暗号方式アルゴリズム（例えば RSA、DSA、ECDSA などがある。）を用いる。このアルゴリズムでは、秘密鍵と公開鍵の 1 組の鍵を持ち、秘密鍵で暗号化したデータは対応する公開鍵でしか復号化出来ない。図 3 に秘密鍵ファイル 3 0 及び公開鍵ファイル 4 0 の内容を示す。秘密鍵ファイル 3 0 には、利用者の ID 番号 3 1、暗証番号 3 2、発行番号 3 3 及び秘密鍵 3 4 が格納されている。公開鍵ファイル 4 0 には、利用者 ID 番号 4 1、発行番号 4 2 及び公開鍵 4 3 が格納されている。秘密鍵と公開鍵の対応関係は発行番号 3 3 および 4 2 によって管理される。

【0026】

発注業務担当者に IC カードあるいはフロッピーディスクに格納された秘密鍵ファイル 3 0 を予め配布し、発注業務担当者は、業務開始前にフロッピーディスクの場合はフロッピーディスク駆動装置、IC カードの場合は IC カードリーダーにそれぞれ記憶媒体をセットする。本実施例ではフロッピーディスク 2 9 で秘密鍵を配布するものとする。

【0027】

業務処理装置 1 において、秘密鍵を作成する方法を図 4 のフローチャートを用いて説明する。秘密鍵ファイルは、複数発注業務担当者がある場合は人数分作成してもよいし、1 つのみ作成し共用してもよい。ここでは、秘密鍵を N 人分作成するとする。

【0028】

ステップ 4 0 1 において全体制御処理プログラム 1 6 0 は鍵作成の指示を操作者から受けると、鍵生成処理制御プログラム 1 6 5 を起動し、ワークエリア 1 6 6 内のプログラムカウンタ K を 0 にセットする。ステップ 4 0 2 において、K に

1 を加算して発行番号をカウントする。ステップ 4 0 3 で K の値と N の値を比較し、 $K \leq N$ ならばステップ 4 0 4 以降の処理を行い、そうでなければ処理を終了する。

【 0 0 2 9 】

ステップ 4 0 4 において鍵生成プログラム 1 6 5 1 を用いてワークエリア 1 6 6 内のメモリに公開鍵暗号方式に基づいた秘密鍵と公開鍵のペアを格納する。公開鍵と秘密鍵のペアは互いに素な 2 つの大きな整数を作り出すことによって得られ、その詳細な作成アルゴリズムは、後藤他、「R A S 暗号鍵高速生成方式」（電子情報通信学会論文誌、D - 1, V o l 7 2 - d - 1, N o 3, p p 2 1 3 - 2 2 0, 1 9 8 9）に開示されている。

【 0 0 3 0 】

ステップ 4 0 5 で利用者 I D 登録プログラム 1 6 5 2 を実行し、キーボード 1 2 から鍵作成担当者が入力した対象とする人の I D 番号 3 1、4 1 と暗証番号 3 2 をワークエリア 1 6 6 のメモリに格納する。暗証番号 3 2 には鍵作成担当者がデフォルト値を設定し、対象者が使用時に暗証番号の変更を行うのが望ましい。

【 0 0 3 1 】

ステップ 4 0 6 において、秘密鍵 F D 作成プログラム 1 6 5 3 を実行し、メモリに格納されたデータを利用して、鍵作成担当者が新しく挿入した秘密鍵格納用フロッピーディスク 2 9 内の秘密鍵ファイル 3 0 に、一人の利用者を示す I D 番号 3 1、デフォルトの暗証番号 3 2、発行番号 3 3 及び公開鍵暗号方式に基づく秘密鍵 3 4 を書き込む。

【 0 0 3 2 】

ステップ 4 0 7 において、公開鍵ファイル作成プログラム 1 6 5 4 を実行し、メモリに格納されたデータを、ネットワークを介してハードディスク 2 4 内の公開鍵ファイル 4 0 上の図 3 に示す利用者 K の I D 番号 4 1、発行番号 4 2 及び公開鍵 4 3 に書き込む。

【 0 0 3 3 】

上記ステップ 4 0 2 から 4 0 7 を利用者全員分（N 個）だけ繰り返すことにより、フロッピーディスクとハードディスクには図 3 の秘密鍵ファイル 3 0 及び公

開鍵ファイル 4 0 に示すような内容が格納される。暗号化のための秘密鍵ファイル 3 0 を格納するフロッピーディスクは、予め業務開始前に発注業務の担当者に配布される。受注業務を行う業務処理装置 2 のハードディスク 2 4 上には N 個の公開鍵が格納されていることになる。

【 0 0 3 4 】

以下、図 5 のフローチャートを用いて、発注データ作成プログラム 1 6 2 の処理を説明する。発注データ作成プログラム 1 6 2 は、(1) 新規に発注書を発行する処理（発注書発行）と、(2) 既に発行済みの発注書を訂正して再発行する処理（発注書訂正再発行）からなる。発注業務担当者から発注業務の開始の指示があった場合、全体制御プログラム 1 6 0 は、発注業務制御プログラム 1 6 1 を起動し、さらに発注業務制御プログラム 1 6 1 は発注データ作成プログラム 1 6 2 を起動する。

【 0 0 3 5 】

ステップ 1 0 1 において、発注データ作成プログラム 1 6 2 は、これから行う業務が (1) 発注書発行業務あるいは (2) 発注書訂正再発行業務のいずれかを発注業務担当者を選択させるための画面をディスプレイ装置 1 1 に表示し、入力を待つ。発注業務担当者は (1) 発注書発行業務か (2) 発注書訂正再発行業務かをキーボード 1 2 あるいはマウス 1 3 を用いて指定する。

【 0 0 3 6 】

ステップ 1 0 2 では、指定された業務が発注書発行業務かどうかを判断する。
1) 発注書発行業務と判断した場合はステップ 1 0 3 へ処理を進める。2) 発注書訂正再発行業務と判断した場合はステップ 1 0 9 へ処理を進める。以下、1) 発注書発行業務の処理内容について説明し、ステップ 1 0 9 ((2) 発注書訂正再発行業務) については後述する。

【 0 0 3 7 】

レイアウト情報格納 DB 1 5 2 には、図 6 に示すような複数の電子文書のレイアウト情報が格納されている。ステップ 1 0 3 ではレイアウト情報格納 DB 1 5 2 を参照し、ディスプレイ 1 1 に電子文書のフォーマット情報を表示し、発注業務担当者にキーボード 1 2 あるいはマウス 1 3 からどの電子文書を使用するのか

を指定させるための画面を表示する。ここでは、図6の発注書A61が選択されたとする。選択されたレイアウトIDは電子文書識別番号として用いられ、ステップ104では、このIDを用いてレイアウト情報格納DB152が参照され、該当するレイアウト情報がワークエリア166上に読み込まれ、ステップ105では、読み込んだレイアウト情報を元に電子文書がディスプレイ11に表示される。レイアウト情報格納DB152の内容を図6の表64に示す。表64では、発注書AのレイアウトIDは“1”である。

【0038】

ステップ106では、画面を元に発注に必要なデータの入力を行う。ここでは、商品番号と必要個数を入力する。日付や発注番号は自動採番でもよいし、担当者の手入力でもよいが、ここでは自動採番とする。発注データ作成プログラム162は、入力されたデータの整合性のチェックや、商品番号を元に商品DB151から商品名を検索・表示するなどの処理を行う。入力の終了した電子文書を図7の発注書A71に示す。

【0039】

発注業務担当者がデータ入力の終了を指示すると、ステップ107において、発注データ作成プログラム162で得られたデータおよび、参照した電子文書名が参照データとして電子文書データ蓄積DB154に登録される。また、通番が採番されて登録される。図8の表83に電子文書データ蓄積DB154の内容を示す。通番831を“1”、参照データ832を“発注書A”、及びデータ833を“107, 20020531, 1215, ミルククッキー, 10, 1326, グルメクッキー, 15”としてそれぞれ登録する。

【0040】

ステップ108で、業務履歴DB153の登録を行う。業務履歴DB153の内容を図8の表82に示す。業務履歴DB153に発注書の発注番号“107”を発注ID821とし、ステップ107で採番した通番（図8のデータ831）を蓄積ID822とし、電子文書の状態823を“発注”としてそれぞれ登録する。

【0041】

次に、図9のフローチャートを用いて、図5のステップ109の(2)発注書訂正再発行を説明する。図7の発注書71の電子文書に対して、発注書訂正再発行を行うものとする。

【0042】

ステップ201において、ディスプレイ11に発注番号入力画面を表示し、発注業務担当者にキーボード12あるいはマウス13から発注書の番号を入力させる。ここでは“発注ID”として“107”を指定したとする。

【0043】

ステップ202において業務履歴DB153を参照し、該当する発注書番号を検索し、該当する蓄積IDを得る。ここでは、“蓄積ID”として“1”を得る。

【0044】

ステップ203において、電子文書データ蓄積DB154からステップ202で得られた蓄積IDと一致する通番を検索し、対応するデータをステップ204でワークエリア166上のメモリに展開（格納）する。ここではデータ“107, 20020531, 1215, ミルククッキー, 10, 1326, グルメクッキー, 15”をメモリ上に展開する。

【0045】

ステップ205において、ステップ203で参照したレコードの参照データの値が通番である場合はステップ203に戻り、対応する通番を再び検索する。参照データの値が電子文書識別番号の場合はステップ206に進む。ここでは“発注書A”となっているので、ステップ206に進み、ワークエリア166上のデータを保存する。

【0046】

ステップ207ではレイアウト情報格納DB152を参照し、ステップ205で得られた電子文書識別番号のレイアウト情報を読み込み、ステップ208でレイアウトを表示する。

【0047】

ステップ209でワークエリア166上に展開されたデータをディスプレイ1

1 上に表示する。

【0048】

ステップ210において、データ、即ち、商品番号と必要個数を入力する。日付や発注番号は自動採番し、入力されたデータの整合性のチェックや、商品番号を元に商品DB151から商品名を検索して表示するなどの処理を行う。入力の終了した電子文書を図7の発注書72に示す。

【0049】

ステップ211において、差分情報を生成する。ステップ206で保存したデータを参照し、画面上のデータとの差分を抽出する。ここではデータ“109, , , , , , 1426, にここにこせんべい, 20”が得られる。差分情報を、ステップ212において電子文書データ蓄積DB154のデータとして追加し（図8のデータ839）、ステップ213において電子文書処理開始時に参照した参照データを登録し（図8のデータ838）、ステップ214において通番を採番（図8のデータ837）して登録する。

【0050】

ステップ215において業務履歴DB153に、発注ID（図8のデータ827）と、ステップ214で採番した通番を蓄積ID（図8のデータ828）として登録し、さらに電子文書の状態に“発注”（図8のデータ829）を登録する。

【0051】

発注データ作成プログラム162終了後、送信データ生成制御プログラム163を実行する。図10のフローチャートを説明する。

【0052】

送信データ生成制御プログラム163は、暗号化する対象データを出来るだけ小さくし、処理時間を短縮するために、注文情報のメッセージダイジェストを生成する場合（ステップ301）、注文情報生成プログラム1631を起動する（ステップ302）。ここでの目的は、ステップ103で指定した発注書のレイアウト情報、入力したデータ、及び発注データ作成プログラム162が生成した商品名、日付及び発注番号からなるワークエリア166上の注文情報に対しメッセ

ージダイジェストを計算することである。データの要約であるメッセージダイジェストに対して暗号化を行えば、処理時間を短縮できる。

【 0 0 5 3 】

ステップ 3 0 3 において注文情報暗号化プログラム 1 6 3 2 が起動され、注文情報あるいはステップ 3 0 1 で計算した注文情報のメッセージダイジェストに対し、発注業務担当者が持つ秘密鍵ファイル 3 0 を使って暗号化を行う。この時、例えば画面上に暗号化確認ボタンを配置し、発注業務担当者によってボタンが押されるまで待つことで、明示的に暗号化を行うことを確認し、確認されたタイミングでフロッピーディスクから秘密鍵を読み込み、暗号化を行っても良い。

【 0 0 5 4 】

注文情報の一部である差分情報を、注文情報を暗号化したものといっしょにパッケージングする場合（ステップ 3 0 4）、ステップ 3 0 5 において、差分情報生成プログラム 1 6 3 3 が起動され、電子文書データ蓄積 DB 1 5 4 の参照データ 8 3 8 及びデータ 8 3 9 が読み込まれ、差分情報が生成される。

【 0 0 5 5 】

注文情報あるいは差分情報を圧縮処理する（ステップ 3 0 6）場合、ステップ 3 0 7 で圧縮処理を行い、ステップ 3 0 8 において送信データ生成プログラム 1 6 3 5 は、注文情報あるいは差分情報とステップ 3 0 3 で得られた暗号化データとを `tar`、`zip` や、`MIME multipart/related` などを用いてパッケージングし、ステップ 3 0 9 において、発注データ送信プログラム 1 6 4 は、ステップ 3 0 8 でパッケージングしたバイナリのデータ列を業務処理装置 2 へ送信する。

【 0 0 5 6 】

次に、業務処理装置 2 の処理を説明する。レイアウト情報格納 DB 2 4 2 は業務処理装置 1 のレイアウト情報格納 DB 1 5 2 と同じ内容を有し、電子文書データ蓄積 DB 2 4 4（図 1 2）は電子文書データ蓄積 DB 1 5 4 と同じ形式を有する。図 1 1 のフローチャートを用いて、図 7 の発注書 7 2 を受信する場合を説明する。

【 0 0 5 7 】

業務処理装置 2 において、受注データ受信プログラム 2 5 2 は常時起動されており、常にデータが受信可能な状態になっている。

【 0 0 5 8 】

ステップ 5 0 1 において業務処理装置 1 からデータを受信すると、ステップ 5 0 2 において受注業務制御プログラム 2 5 1 は受信データ解析制御プログラム 2 5 3 を起動し、さらに、受信データ解析制御プログラム 2 5 3 は受信データ分割プログラム 2 5 3 1 を起動する。ここでは、業務処理装置 1 から受信したデータを注文情報あるいは差分情報と暗号化データとに分割する。

【 0 0 5 9 】

ステップ 5 0 3 において注文情報あるいは差分情報に圧縮処理が施されている場合は、圧縮復元プログラム 2 5 3 4 で伸長処理を行う（ステップ 5 0 4）。

【 0 0 6 0 】

次に、注文情報生成プログラム 2 5 3 2 において、注文情報を生成する。受信したデータが差分情報であった場合（ステップ 5 0 5）、ステップ 5 0 6 において、ステップ 5 0 2 で得られた差分情報あるいはステップ 5 0 4 で伸長処理した差分データから参照データ及びデータを抽出し、電子文書データ蓄積 DB 2 4 4 の参照データ 1 2 8 及びデータ 1 2 9 に登録する。参照データ 1 2 8 の値は“1”、データ 1 2 9 の値は“1 0 9, , , , , , 1 4 2 6, にここにこせんべい, 2 0”である。さらに、データ 1 2 9 の値をワークエリア 2 5 5 に書き込む。

【 0 0 6 1 】

ステップ 5 0 7 において、参照データ 1 2 8 の値は“1”なので、通番“1”となっているレコードを検索して、ステップ 5 0 8 において、通番“1”に対応するデータ 1 2 3 の値を参照し、ワークエリア 2 5 5 にマージする。ここでは、マージした結果は“1 0 9, 2 0 0 2 0 5 3 1, 1 2 1 5, ミルククッキー, 1 0, 1 3 2 6, グルメクッキー, 1 5, 1 4 2 6, にここにこせんべい, 2 0”となる。

【 0 0 6 2 】

ステップ 5 0 9 において、参照データ 1 2 2 が通番の場合はステップ 5 0 7 に戻り、電子文書識別番号の場合はステップ 5 1 0 に進み、該当するレイアウト情

報格納DB 2 4 2を読み込む。ここでは参照データ1 2 2が“発注書A”となっているので、レイアウト格納情報DB 2 4 2を参照し、“発注書A”のフォーマット情報をワークエリア2 5 5に読み込み、注文情報の生成を終了する。ここでの注文情報は、発注書Aのフォーマット情報と、ステップ5 0 8で生成した値“1 0 9, 2 0 0 2 0 5.3 1, 1 2 1 5, ミルククッキー, 1 0, 1 3 2 6, ゲルメクッキー, 1 5, 1 4 2 6, にこにこせんべい, 2 0”である。ステップ5 1 1において公開鍵ファイル4 0を参照し、暗号化データを復号化する。

【0 0 6 3】

復号化したデータがメッセージダイジェストの場合（ステップ5 1 2）、ステップ5 1 3において注文情報のメッセージダイジェストを算出し、ステップ5 1 4において、ステップ5 1 3で得られたメッセージダイジェストとステップ5 1 1で復号化したメッセージダイジェストとの比較、あるいは注文情報とステップ5 1 1で復号化した注文情報との比較を行って、改竄があったか否かを検定する。

【0 0 6 4】

データが一致した場合は、業務処理装置1において発注業務担当者が発注データ作成プログラム1 6 2によって作成した注文情報と、業務処理装置2において注文情報生成プログラム2 5 3 2が生成された注文情報とが一致したことになるため、注文情報が確かに発注業務担当者によって作成されたものであると判断し、一致しなかった場合は、注文情報は発注業務担当者によって作成されたものではないことになる。

【0 0 6 5】

【発明の効果】

発注書に対して暗号化を行うことにより、オリジナル部分の改竄が行われても、容易に改竄を検出でき、安全な電子商取引を行うことができる。

【図面の簡単な説明】

【図1】

ハードウェア構成図である。

【図2】

ソフトウェア構成図である。

【図 3】

秘密鍵ファイルおよび公開鍵ファイルの構造である。

【図 4】

鍵作成のためのフローチャートである。

【図 5】

発注データ作成プログラムの処理フローチャートである。

【図 6】

レイアウト情報格納 DB である。

【図 7】

発注書の入力例である。

【図 8】

業務処理装置 1 の業務履歴 DB および電子文書データ蓄積 DB である。

【図 9】

発注書訂正再発行の処理フローチャートである。

【図 1 0】

送信データ生成制御プログラムの処理フローチャートである。

【図 1 1】

業務処理装置 2 における発注書受信後の処理フローチャートである。

【図 1 2】

業務処理装置 2 の電子文書データ蓄積 DB である。

【図 1 3】

本発明の業務概略図である。

【符号の説明】

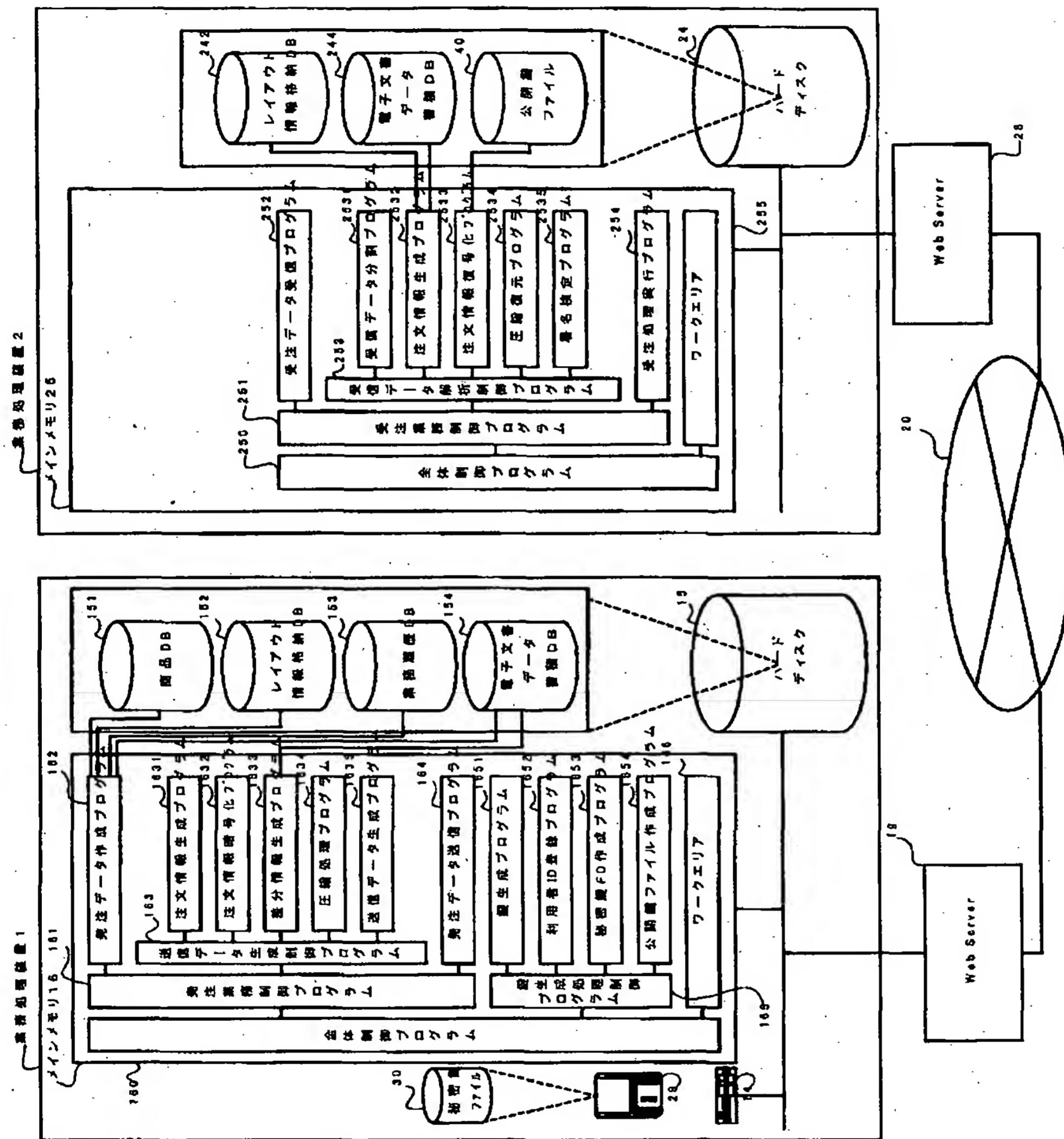
1 : 業務処理装置, 2 : 業務処理装置, 1 1 : ディスプレイ, 1 2 : キーボード
, 1 3 : マウス, 1 4 : フロッピーディスク駆動装置, 1 5 : ハードディスク
, 1 6 : メインメモリ, 1 7 : CPU, 1 8 : バス, 1 9 : サーバ, 2 0 : イン
ターネット, 2 1 : ディスプレイ, 2 2 : キーボード, 2 3 : マウス, 2 4 : ハ
ードディスク, 2 5 : メインメモリ, 2 6 : CPU, : 2 7 バス, 2 8 : サーバ

， 2 9 : フロッピーディスク， 3 0 : 秘密鍵（暗号化鍵）ファイル， 1 6 0 : 全
体制御プログラム， 1 6 1 : 発注業務制御プログラム， 1 6 2 : 発注データ作成
プログラム， 1 6 3 : 送信データ生成制御プログラム

【書類名】 図面

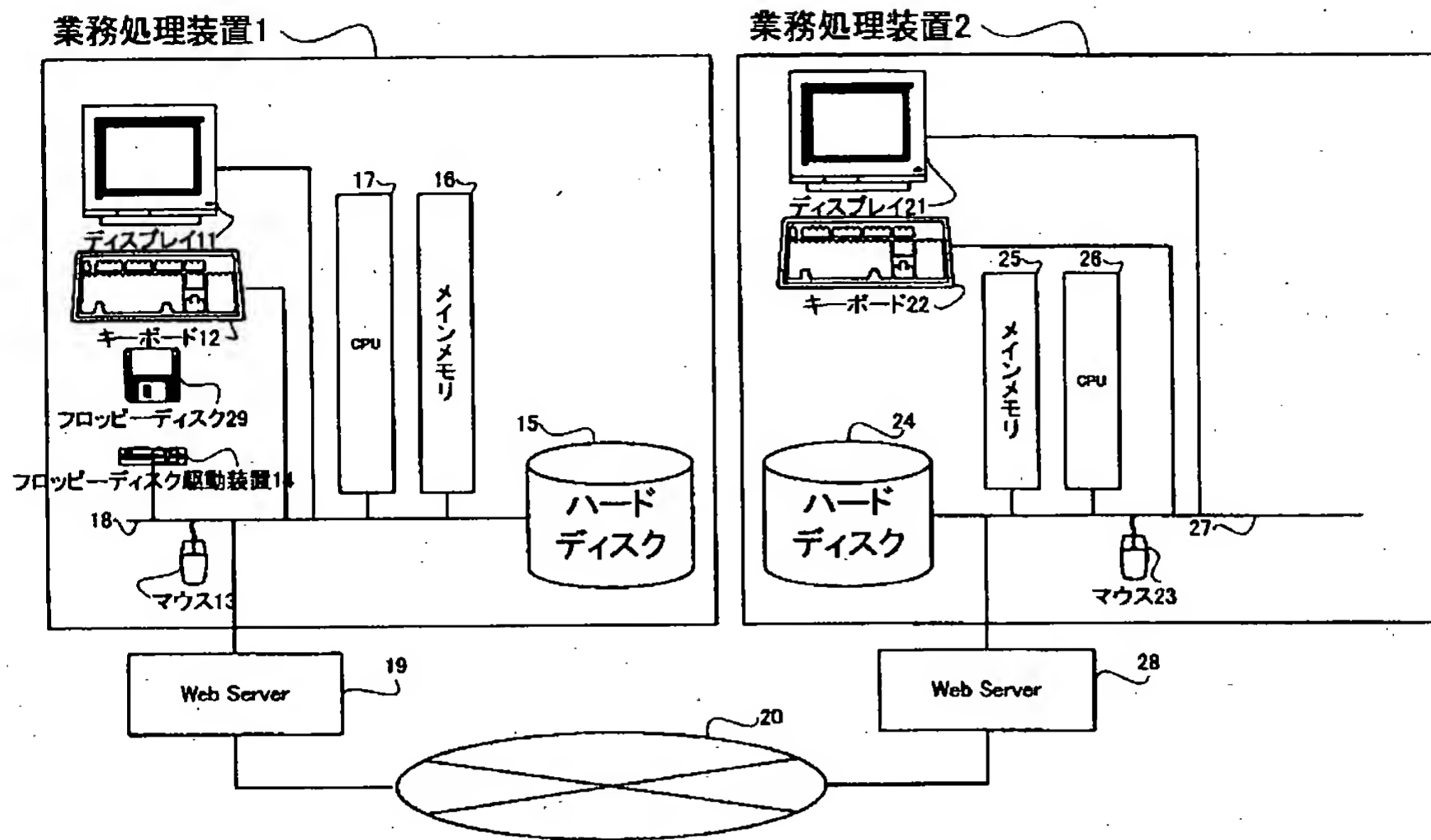
【図1】

図1



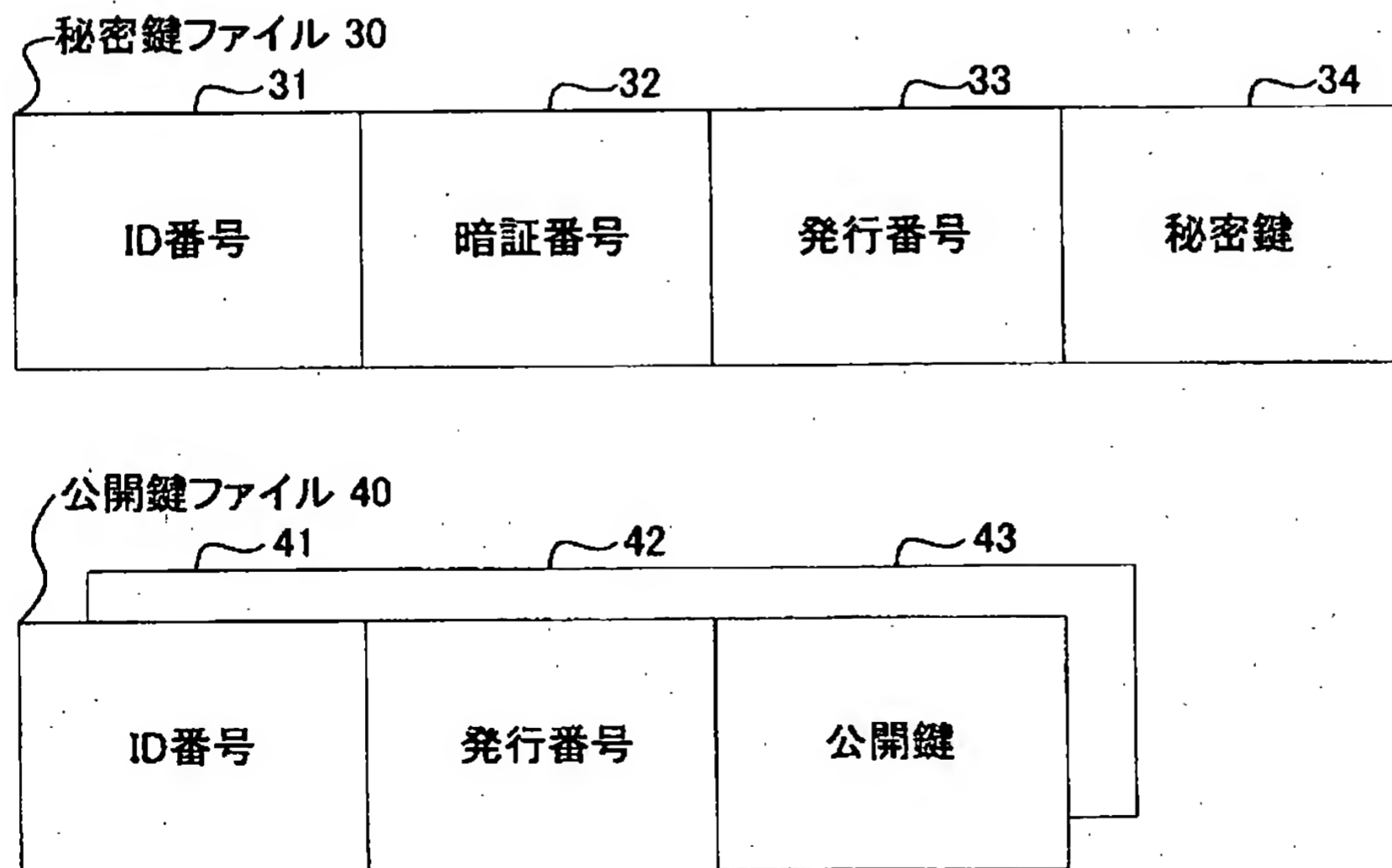
【図2】

図2



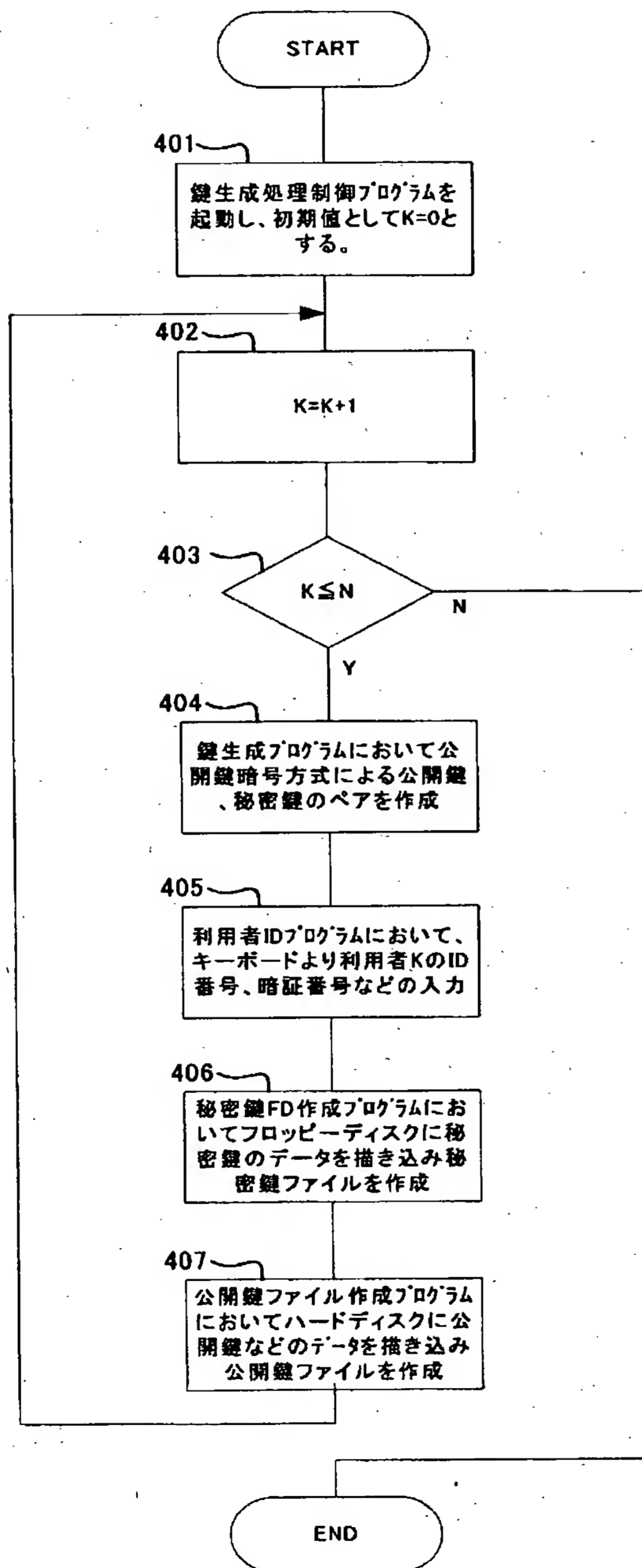
【図3】

図3



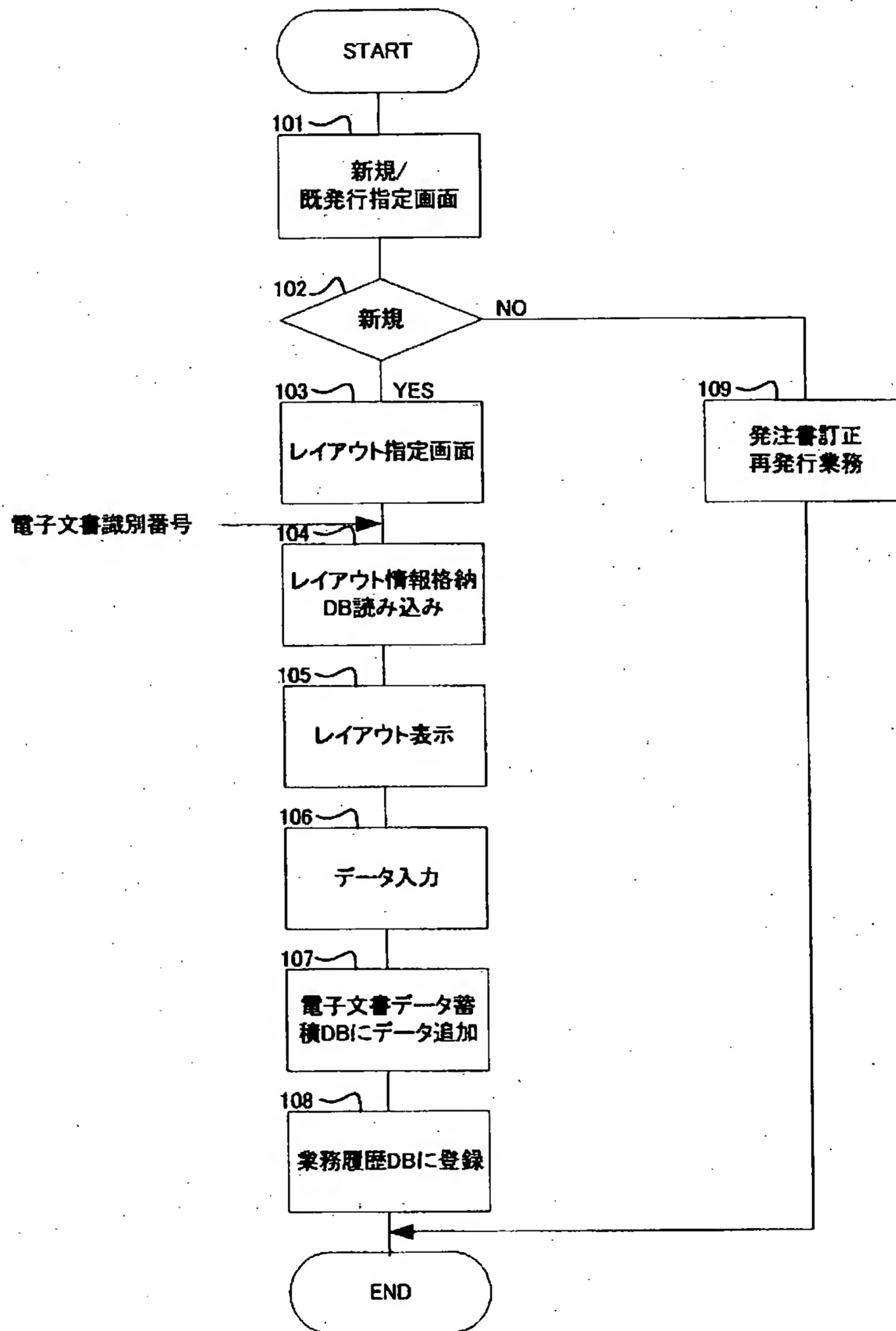
【図4】

図4



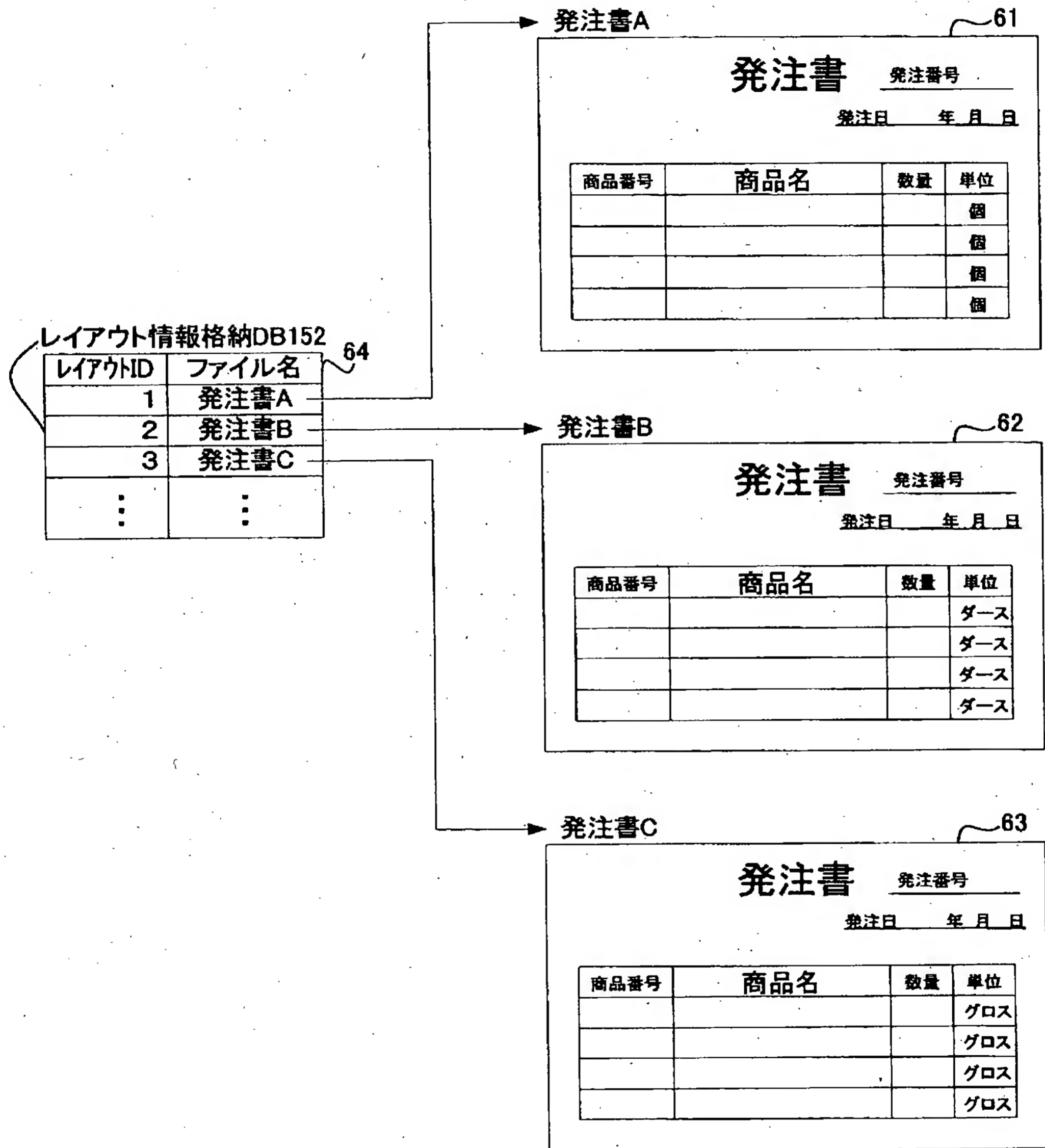
【図 5】

図 5



【図 6】

図 6



【図 7】

図 7

発注書A

71

発注書			
		発注番号 107	
発注日 2002 年 月 日			
商品番号	商品名	数量	単位
1215	ミルクチョコレート	10	個
1326	グルメクッキー	15	個
			個
			個
			個

発注書A

72

発注書			
		発注番号 109	
発注日 2002 年 月 日			
商品番号	商品名	数量	単位
1215	ミルクチョコレート	10	個
1326	グルメクッキー	15	個
1426	にこにこせんべい	20	個
			個
			個

【図 8】

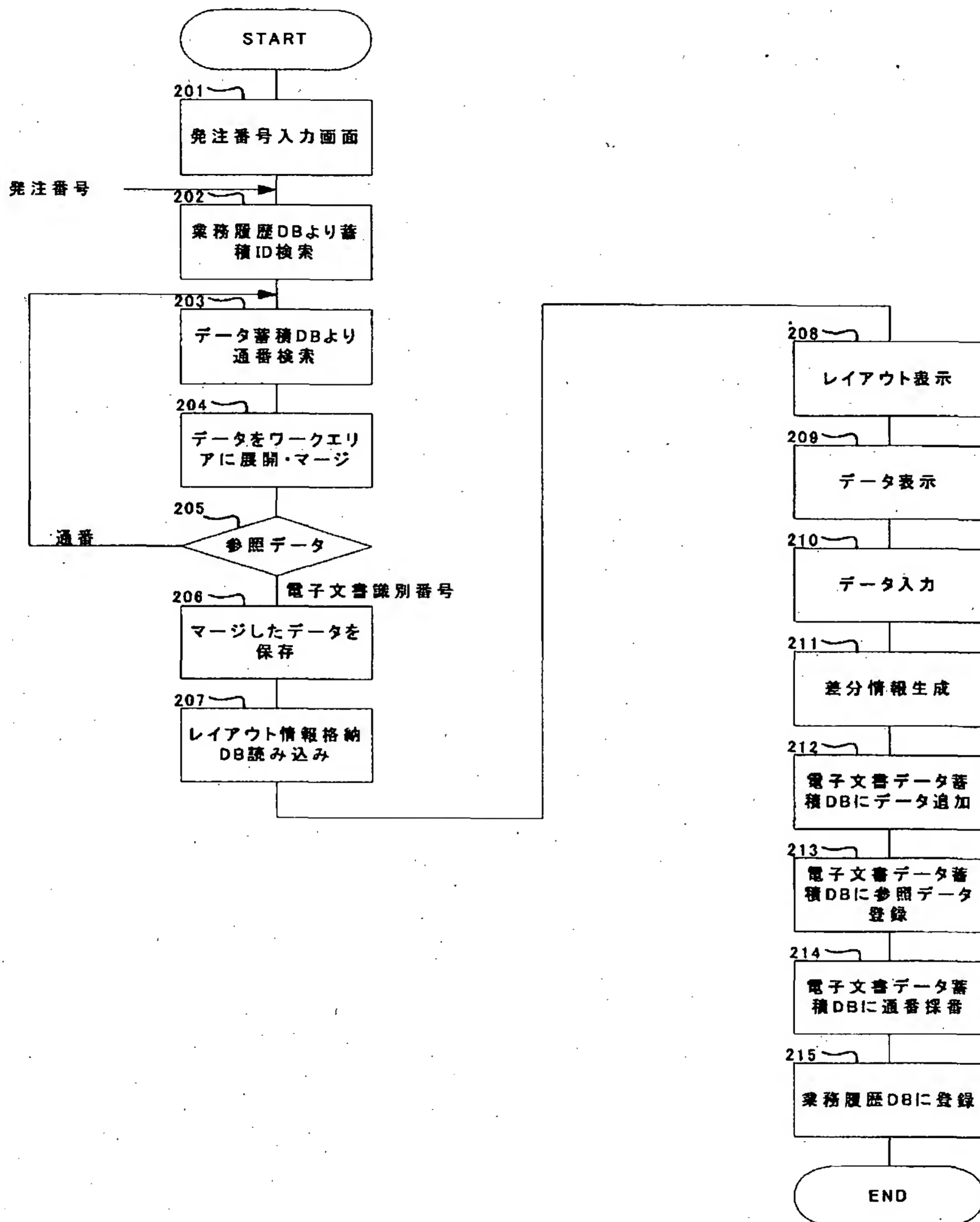
図 8

業務履歴DB153			
発注ID	蓄積ID	状態	
107	1	発注	
108	2	発注	
109	3	発注	

電子文書データ蓄積DB154		
通番	参照データ	データ
1	発注書A	107,20020531,1215,ミルククッキー,10,1326,グルメクッキー,15
2	発注書B	108,20020531,2115,かきかた鉛筆,10,2226,サインペン,10
3	1	109.....,1426,にこにこせんべい,20

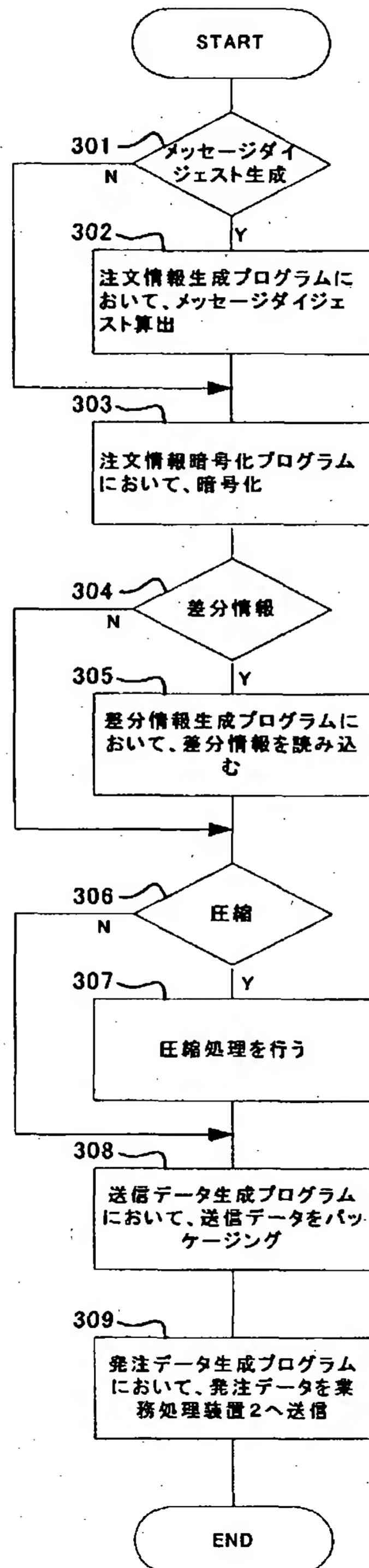
【図9】

図9



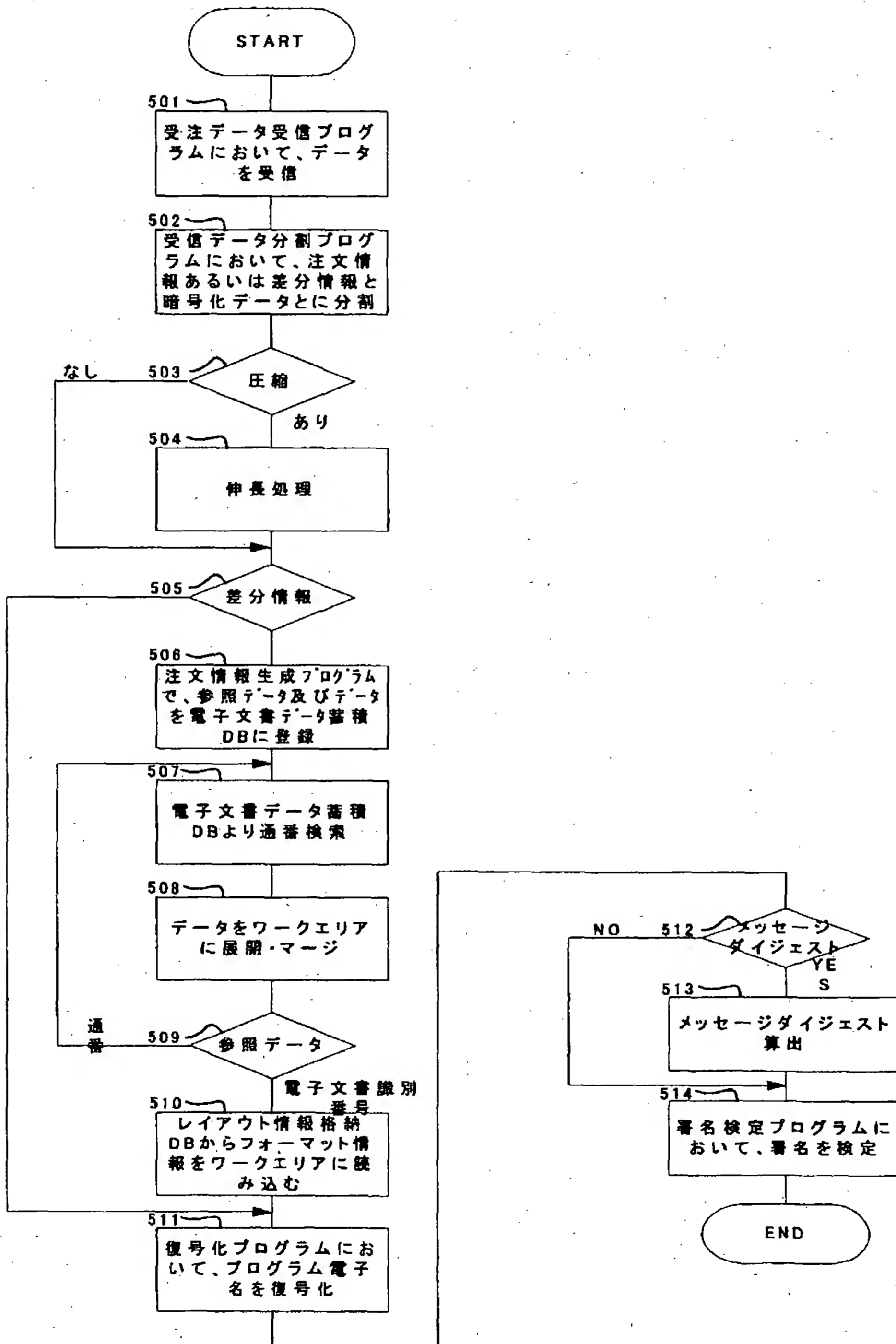
【図10】

図10



【図 11】

図 11



【図 1 2】

図 1 2

電子文書データ蓄積DB244

通番	参照データ	データ
121 1	発注書A	107,20020531,1215,ミルククッキー,10,1326,グルメクッキー,15
124 2	発注書B	108,20020531,2115,かきかた鉛筆,10,2226,サインペン,10

122

123

126

125

電子文書データ蓄積DB244

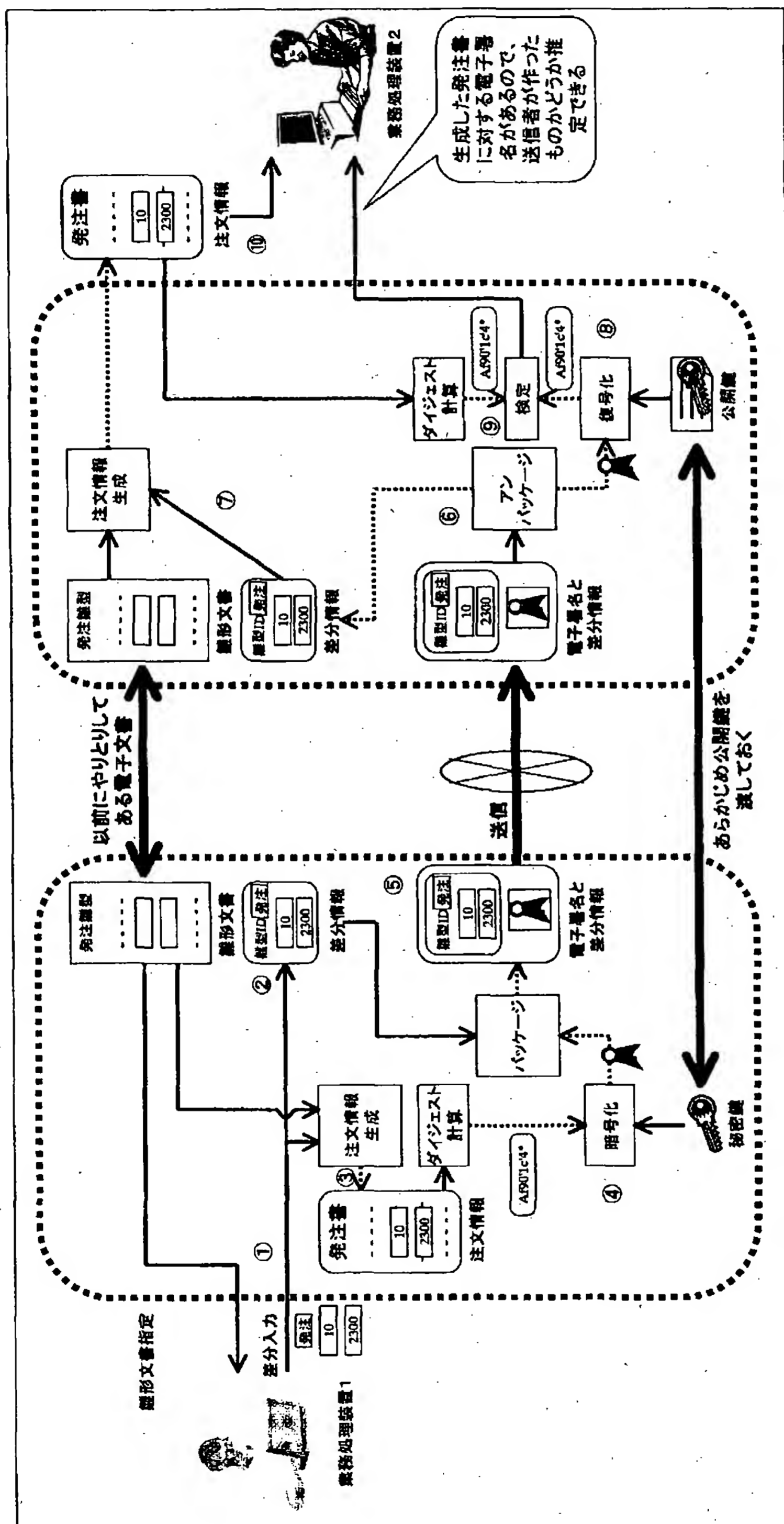
通番	参照データ	データ
1	発注書A	107,20020531,1215,ミルククッキー,10,1326,グルメクッキー,15
2	発注書B	108,20020531,2115,かきかた鉛筆,10,2226,サインペン,10
3	1	109,.....,1426,にこにこせんべい,20

127

128

129

【図 13】



【書類名】 要約書

【要約】

【課題】

電子商取引において、単純に差分に電子署名を付した場合は、受信者は差分が送信者によって作成されたことしか推定できないため、生成した電子文書に対して署名検定ができない。

【解決手段】

2 台の装置に共通する雛形データを予め記憶させ、データを送信する装置は、オリジナル情報を暗号化し、差分情報を生成し、暗号化したオリジナル情報と差分情報をパッケージ化し、データを受信する装置は、受信したデータをアンパッケージし、差分情報と雛形データからオリジナル情報を復元し、暗号化したデータを復号化し、復号化したデータと復元したオリジナル情報が一致するか否かを判定する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願2002-294375
受付番号	50201510676
書類名	特許願
担当官	第七担当上席 0096
作成日	平成14年10月 9日

<認定情報・付加情報>

【提出日】	平成14年10月 8日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所